Nom : _____ Date : _____ Note : _____

Sécurité et chiffrement du Wi-Fi public

Attaques de l'homme du milieu, points d'accès pirates, reniflage de paquets, tunnels VPN et chiffrement HTTPS.

PRÉSENTATION DE L'APPRENTISSAGE : SÉCURITÉ DU WI-FI PUBLIC

SÉCURISÉ
CHIFFREMENT DES DONNÉES
Norme AES 256 bits

CONFORME
NORMES MONDIALES
Cadres RGPD (GDPR) et CCPA

ZERO TRUST
POLITIQUE D'ACCÈS
Authentification multifacteur

Bienvenue ! Ce dossier d'activités vous guide à travers les Wi-Fi publics et leur sécurité. Vous étudierez les réseaux non chiffrés, les attaques de l'homme du milieu (MitM), les points d'accès malveillants, le reniflage de paquets, les tunnels VPN et la sécurité des échanges en HTTPS.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la cybersécurité

URL: https://www.vpn.com/fr/cybersecurite/securite-wifi-public/

Votre parcours d'apprentissage : sécurité du Wi-Fi public

- Identifier les risques courants des Wi-Fi publics, notamment le reniflage de paquets et les points d'accès malveillants.
- Mettre en place des tunnels de chiffrement VPN pour sécuriser les données en transit.
- Imposer HTTPS et des paramètres de navigateur web sécurisés pour les employés à distance.

CONSIGNES DU GUIDE SUR LA SÉCURITÉ DU WI-FI PUBLIC

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à la sécurité de l'accès à distance. Terminez par l'activité bonus Réflexion rapide.

SÉCURITÉ DU WI-FI PUBLIC ET PROTECTION EN TRANSIT (INTRODUCTION)

Les points d'accès Wi-Fi publics non chiffrés exposent le trafic réseau à l'interception de paquets (sniffing) et à l'usurpation de type Evil Twin. Faire passer le trafic par des tunnels VPN chiffrés et imposer des règles HSTS HTTPS uniquement protège les sessions contre l'interception sur le réseau local.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Qu'est-ce qu'une attaque de l'homme du milieu (MitM) ?

- A. Intercepter et modifier les communications entre deux parties sur un réseau partagé
- B. Une technique d'extraction de base de données visant les enregistrements d'utilisateurs
- C. Submerger les serveurs web de requêtes de trafic réseau
- D. Effacer les volumes de stockage du disque dur local

2. Qu'est-ce qu'un point d'accès malveillant (Evil Twin) ?

- A. Un point d'accès Wi-Fi malveillant configuré avec le même SSID qu'un réseau légitime
- B. Un outil d'administration utilisé pour surveiller les sauvegardes de base de données
- C. Une configuration de passerelle VPN sécurisée
- D. Un enregistrement DNS qui recense les serveurs de messagerie autorisés

3. Comment un VPN protège-t-il le trafic sur un Wi-Fi public ?

- A. Il enveloppe tous les paquets réseau dans un tunnel chiffré, ce qui les rend illisibles pour les renifleurs
- B. Il bloque automatiquement toutes les demandes de connexion entrantes
- C. Il modifie l'adresse MAC de la carte réseau physique
- D. Il supprime les cookies mis en cache dans le navigateur

4. Qu'est-ce que le reniflage de paquets (packet sniffing) ?

- A. Utiliser des outils matériels ou logiciels pour capturer et enregistrer les paquets réseau
- B. Analyser les répertoires locaux à la recherche de fichiers en double
- C. Restreindre les droits de lecture de la base de données selon les rôles des utilisateurs
- D. Chiffrer les disques de stockage avec des clés AES-256

5. Quel est le rôle de HTTPS ?

- A. Chiffrer le trafic de la session entre le navigateur et le serveur web
- B. Filtrer les e-mails entrants au niveau de la passerelle
- C. Compresser les images pour accélérer le chargement des pages
- D. Gérer l'arborescence des fichiers d'un stockage en réseau (NAS)

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Les utilisateurs connectés peuvent facilement capturer des données en clair sur les réseaux Wi-Fi publics ouverts.

- ◯ Vrai
- ◯ Faux

7 Question 7

7. Les points d'accès malveillants (Evil Twins) sont toujours autorisés par les administrateurs réseau.

- ◯ Vrai
- ◯ Faux

8 Question 8

8. Un VPN est inefficace pour protéger le trafic contre l'écoute de paquets (sniffing) sur les réseaux publics.

- ◯ Vrai
- ◯ Faux

9 Question 9

9. HTTPS ne chiffre que le chemin de l'URL et laisse le contenu des paquets en clair.

- ◯ Vrai
- ◯ Faux

10 Question 10

10. Les points d'accès Wi-Fi utilisant la sécurité WPA3 offrent une meilleure protection que les réseaux ouverts sans mot de passe.

- ◯ Vrai
- ◯ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Capturer des mots de passe privés sur un Wi-Fi public relève de l' _____ des communications.

2. Analyser des paquets bruts sur un réseau local relève du _____ de paquets.

3. Un point d'accès malveillant imitant le Wi-Fi d'un hôtel est un _____ .

4. Sécuriser le transit du trafic web exige un chiffrement par _____ .

5. Chiffrer toutes les sorties réseau fait appel à un _____ .

6. Un chemin de communication chiffré à travers les réseaux publics est un _____ .

BANQUE DE MOTS DE VOCABULAIRE

CLIENT VPN HTTPS INTERCEPTION JUMEAU MALÉFIQUE NORME WPA
PARE-FEU RENIFLAGE TUNNEL

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur la sécurité

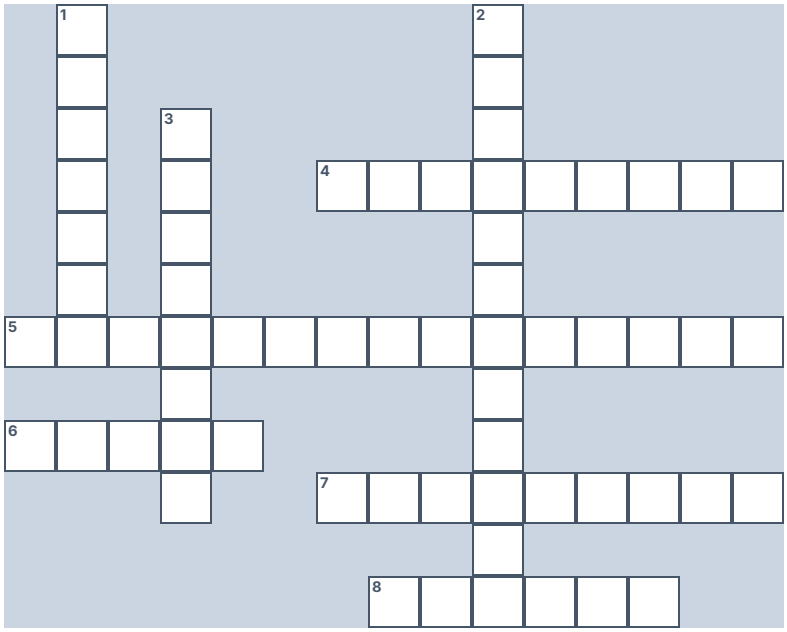
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. INTERCEPTION	A	Norme de sécurité Wi-Fi moderne.
☐	2. INTERCEPTION DE PAQUETS	B	Chemin sécurisé des données en transit.
☐	3. JUMEAU MALVEILLANT	C	Filtrage du trafic entrant.
☐	4. HTTPS	D	Point d'accès malveillant imitant un Wi-Fi.
☐	5. VPN	E	Lecture du trafic en transit.
☐	6. TUNNEL	F	Capture des paquets de données réseau.
☐	7. WPA3	G	Réseau privé virtuel chiffré.
☐	8. PARE-FEU	H	Transmission web sécurisée.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

4. Réseau privé virtuel chiffré. (9)

5. Point d'accès malveillant imitant un réseau Wi-Fi. (15)

6. Transmission web sécurisée. (5)

7. Capture des paquets de données réseau. (9)

8. Chemin sécurisé des données en transit. (6)

VERTICALEMENT

1. Filtrage du trafic entrant. (7)

2. Lecture du trafic en transit. (12)

3. Norme moderne de sécurité Wi-Fi (WPA3). (8)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

4 horizontal: Réseau privé virtuel chiffré. (9 lettres):

5 horizontal: Point d'accès malveillant imitant un réseau Wi-Fi. (15 lettres):

6 horizontal: Transmission web sécurisée. (5 lettres):

7 horizontal: Capture des paquets de données réseau. (9 lettres):

8 horizontal: Chemin sécurisé des données en transit. (6 lettres):

VERTICALEMENT

1 vertical: Filtrage du trafic entrant. (7 lettres):

2 vertical: Lecture du trafic en transit. (12 lettres):

3 vertical: Norme moderne de sécurité Wi-Fi (WPA3). (8 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

P N C U B A Z J N D K A D O D
F P H I D R Q U M E I I R Z S
F V Q V F A A M Q O N N P T X
Q T K R U S D E N Y T B F S X
E N W J A R Z A Y Y E L G I M
G E R J M L T U O H R Q Q H Z
A I A O T N V M G U C B Y R Y
L L B H U O L A Z G E J O P N
F C W C N R M L Z Y P G U Y O
I W U K N M V E P B T N E H V
N T M G E E V F D Y I U F T K
E R B X L W Z I Y M O R E T Q
R X I P D P A Q D J N Q R P V
W W L J H A T U H G B E A S I
K T S V R Z E E H E S C P A L

LISTE DE MOTS DE VOCABULAIRE

INTERCEPTION RENIFLAGE JUMEAUMALEFIQUE HTTPS CLIENTVPN TUNNEL NORMEWPA PAREFEU

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. INTERCEPTION
B. RENIFLAGE
C. JUMEAUMALEFIQUE
D. HTTPS
E. CLIENTVPN
F. TUNNEL
G. NORMEWPA
H. PAREFEU

DÉFINITIONS ET CHAMPS D'ASSOCIATION
_____ 1. Norme moderne de sécurité Wi-Fi (WPA3).
_____ 2. Point d'accès malveillant imitant un réseau Wi-Fi.
_____ 3. Capture des paquets de données réseau.
_____ 4. Chemin sécurisé des données en transit.
_____ 5. Filtrage du trafic entrant.
_____ 6. Lecture du trafic en transit.
_____ 7. Réseau privé virtuel chiffré.
_____ 8. Transmission web sécurisée.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. T C P R N E I I O T N E
2. U U E M M A Q J E U E F I L A
3. C T N L V N E P I
4. M P A W E N O R
5. A F E E L I R G N
6. P H T S T
7. E T N L N U
8. A E U P E F R

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Raisons de mettre à jour les logiciels			
2	Appareils qui se connectent automatiquement au Wi-Fi			
3	Informations que vous ne devriez jamais partager			
4	Bonnes habitudes de sécurité à adopter dès aujourd'hui			
5	Façons de rester en sécurité dans un café			
6	Appareils qui peuvent être piratés			
7	Choses qu'un pirate peut voir sur un Wi-Fi ouvert			
8	Signes d'un faux réseau Wi-Fi			
9	Alternatives au Wi-Fi public			
10	Signaux d'alerte dans un e-mail			
11	Choses que vous ne faites pas sur un Wi-Fi public			
12	Endroits avec un Wi-Fi gratuit			
13	Façons de protéger vos comptes			
14	Signes qu'un ordinateur est infecté			
15	Noms de Wi-Fi qui semblent suspects			

Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : CONTENIR L'INTERCEPTION DE PAQUETS SUR UN WI-FI PUBLIC

👷

Scénario : Un commercial à distance, connecté au réseau Wi-Fi public d'un aéroport, remarque que plusieurs e-mails professionnels sensibles ont fuité peu après leur envoi en clair.

Question de discussion : Analysez les risques des réseaux publics et décrivez une solution de chiffrement du trafic.

ÉTUDE DE CAS 2 : DÉFENSE CONTRE LES FAUX POINTS D'ACCÈS EVIL TWIN

👷

Scénario : Des attaquants déploient un point d'accès sans fil malveillant nommé 'CoffeeShop_Guest' qui imite le point d'accès légitime d'un café, et capturent le trafic réseau de clients qui ne se doutent de rien.

Question de discussion : Détaillez les étapes de vérification permettant de détecter et de bloquer les points d'accès malveillants.

Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

3	8	9	6	6	18	5	26		12	5		20	18	1	6	9	3

23	9	6	9		16	21	2	12	9	3		1	22	5	3		21	14

22	16	14

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q1: Pourquoi le Wi-Fi public n'est-il pas sécurisé ?

Un Wi-Fi public ouvert ne chiffre pas le trafic sur les ondes : d'autres personnes à proximité peuvent donc capter toute donnée non protégée. [2]

Q2: Qu'est-ce que la capture de paquets (packet sniffing) ?

Un renifleur de paquets (packet sniffer) capture les données brutes qui circulent sur une interface réseau, ce qui expose les mots de passe en clair et les détails du trafic.

Q3: Qu'est-ce qu'un Evil Twin ?

Un point d'accès malveillant installé par des pirates, qui imite le nom et les paramètres d'un point d'accès Wi-Fi local de confiance.

Q4: Comment un VPN me protège-t-il ?

Il fait passer votre trafic par un tunnel chiffré, ce qui masque votre activité de navigation aux renifleurs du réseau local.

Q5: Le HTTPS me protège-t-il sur un Wi-Fi public ?

Oui, il chiffre les données échangées entre votre navigateur et le site web, et un VPN ajoute une couche de protection supplémentaire.

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q6: Qu'est-ce que le WPA3 ?

La norme Wi-Fi Protected Access moderne, qui offre un chiffrement plus solide et une protection contre les attaques par dictionnaire hors ligne. [1]

Q7: Un Wi-Fi public peut-il transmettre des logiciels malveillants ?

Oui, les attaquants peuvent intercepter le trafic et injecter dans votre session de navigation des invites de téléchargement malveillantes (téléchargements furtifs, ou drive-by downloads).

Q8: Quel est le risque du partage de fichiers ?

Si le partage de fichiers est activé, d'autres utilisateurs du réseau public peuvent lire ou modifier vos dossiers locaux.

Q9: Qu'est-ce qu'un portail captif ?

La page de connexion qu'utilisent les réseaux des hôtels ou des cafés pour accorder l'accès à Internet, et que des attaquants peuvent parfois usurper.

Q10: Faut-il désactiver le Wi-Fi quand on ne l'utilise pas ?

Oui, désactiver le Wi-Fi empêche votre appareil de se connecter automatiquement à des réseaux non fiables.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q1: Comment une attaque de l'homme du milieu exploite-t-elle le DNS ?

En utilisant l'usurpation DNS sur un routeur malveillant pour diriger les navigateurs ciblés vers des pages d'hameçonnage ressemblantes au lieu des domaines visés.

Q2: Qu'est-ce que le détournement de session ?

Un attaquant qui intercepte un cookie de session non chiffré sur un Wi-Fi public et l'importe pour contourner la connexion par identifiants.

Q3: Qu'est-ce que le SSL stripping ?

Une attaque de l'homme du milieu (MitM) dans laquelle l'attaquant rétrograde la requête HTTPS sécurisée d'un utilisateur en HTTP non chiffré, ce qui lui permet de capturer les identifiants en clair.

Q4: Comment HSTS protège-t-il contre le SSL stripping ?

HTTP Strict Transport Security oblige les navigateurs à se connecter uniquement en HTTPS, en refusant tout repli vers HTTP non chiffré. [3]

Q5: Qu'est-ce qu'un VPN à tunnel partagé (split tunnel) ?

Une configuration qui n'achemine que le trafic de l'entreprise par le VPN et envoie directement les données Internet publiques, ce qui peut exposer à des risques de fuite.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q6: Pourquoi le WPA2 est-il vulnérable à KRACK ?

L'attaque par réinstallation de clé (KRACK) exploite la poignée de main en quatre étapes de WPA2 pour déchiffrer des paquets sans le mot de passe Wi-Fi.

Q7: Qu'est-ce que l'isolation des clients ?

Un paramètre de sécurité du routeur qui empêche les appareils Wi-Fi connectés de communiquer directement entre eux, ce qui bloque l'écoute locale.

Q8: Comment les attaquants utilisent-ils de faux serveurs DNS ?

Ils configurent des routeurs malveillants qui attribuent de faux serveurs DNS aux clients, ce qui leur permet d'intercepter et de réécrire toutes les résolutions web.

Q9: Un VPN peut-il masquer mon adresse MAC locale ?

Non. Les adresses MAC sont des identifiants locaux de couche 2 ; utilisez plutôt le paramètre de randomisation MAC (adresse privée) intégré à votre appareil.

Q10: Qu'est-ce qu'une attaque par usurpation de portail captif ?

Un attaquant qui héberge un faux portail d'authentification sur un point d'accès malveillant pour voler des identifiants sous prétexte d'un accès Wi-Fi gratuit.

Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

1. APERÇU SÉCURITÉ

Les travailleurs à distance utilisent souvent le Wi-Fi des cafés, des hôtels et des aéroports, où ils ne peuvent pas contrôler la sécurité du réseau.

2. APERÇU SÉCURITÉ

Un point d'accès malveillant de type « jumeau maléfique » (Evil Twin) peut copier exactement le nom et l'adresse MAC d'un réseau de confiance, ce qui trompe les appareils.

3. APERÇU SÉCURITÉ

Les logiciels de capture de paquets comme Wireshark sont gratuits et peuvent afficher en clair les mots de passe HTTP non chiffrés.

4. APERÇU SÉCURITÉ

La sécurité WPA3 utilise SAE (Simultaneous Authentication of Equals) pour se protéger contre les attaques locales par force brute.

5. APERÇU SÉCURITÉ

Les attaques par SSL stripping contournent les protections HTTPS de base en interceptant les premières redirections HTTP au niveau de la passerelle.

6. APERÇU SÉCURITÉ

Les en-têtes de réponse HTTP Strict Transport Security (HSTS) empêchent les navigateurs de revenir à des connexions HTTP non chiffrées. [3]

7. ZOOM SUR LA SÉCURITÉ

Désactiver la 'connexion automatique' empêche les smartphones de se connecter à des réseaux malveillants imitant des réseaux légitimes dans les lieux publics.

8. ZOOM SUR LA SÉCURITÉ

Les configurations VPN d'entreprise « toujours actives » font passer tout le trafic réseau des employés à distance par les pare-feu de l'entreprise.

9. ZOOM SUR LA SÉCURITÉ

Les points d'accès malveillants peuvent fournir de fausses réponses DNS et rediriger les domaines ciblés vers des serveurs d'hameçonnage.

10. APERÇU SÉCURITÉ

Sans VPN, les autres utilisateurs d'un point d'accès ouvert peuvent voir quels sites et quels serveurs votre appareil contacte.

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce qu'une attaque de l'homme du milieu (MitM) ? → Intercepter et modifier les communications entre deux parties sur un réseau partagé

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce qu'un point d'accès malveillant (Evil Twin) ? → Un point d'accès Wi-Fi malveillant configuré avec le même SSID qu'un réseau légitime

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Comment un VPN protège-t-il le trafic sur un Wi-Fi public ? → Il enveloppe tous les paquets réseau dans un tunnel chiffré, ce qui les rend illisibles pour les renifleurs

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce que le reniflage de paquets (packet sniffing) ? → Utiliser des outils matériels ou logiciels pour capturer et enregistrer les paquets réseau

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quel est le rôle de HTTPS ? → Chiffrer le trafic de la session entre le navigateur et le serveur web

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les utilisateurs connectés peuvent facilement capturer des données en clair sur les réseaux Wi-Fi publics ouverts.

7 Question 7

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : un Evil Twin est un point d'accès non autorisé installé par un attaquant pour imiter un point d'accès réel.

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : un VPN chiffre le trafic dans un tunnel, de sorte que les renifleurs locaux ne peuvent pas le lire.

9 Question 9

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : HTTPS chiffre l'ensemble de l'échange HTTP, y compris le chemin de l'URL et le contenu de la page.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les points d'accès Wi-Fi utilisant la sécurité WPA3 offrent une meilleure protection que les réseaux ouverts sans mot de passe.

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

E 1. INTERCEPTION	F 2. INTERCEPTION DE PAQUETS	D 3. JUMEAU MALVEILLANT	H 4. HTTPS
G 5. VPN	B 6. TUNNEL	A 7. WPA3	C 8. PARE-FEU

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 INTERCEPTION	2 RENIFLAGE	3 JUMEAU MALÉFIQUE	4 HTTPS
5 CLIENT VPN	6 TUNNEL		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 G – NORMEWPA	2 C – JUMEAUMALEFIQUE	3 B – RENIFLAGE	4 F – TUNNEL
5 H – PAREFEU	6 A – INTERCEPTION	7 E – CLIENTVPN	8 D – HTTPS

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer INTERCEPTION, INTERCEPTION DE PAQUETS et JUMEAU MALVEILLANT avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

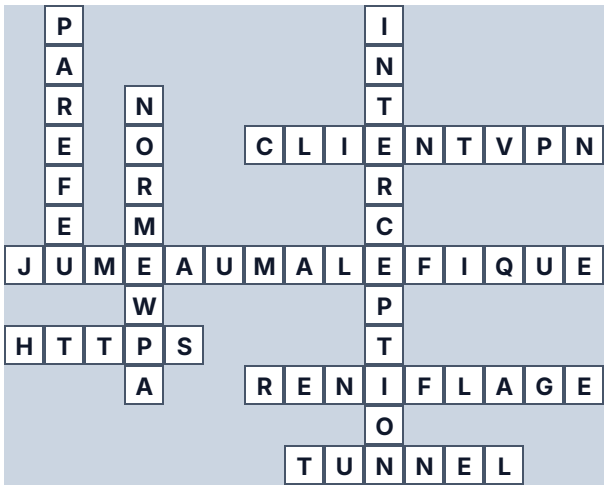
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

P	N	C	U	B	A	Z	J	N	D	K	A	D	O	D
F	P	H	I	D	R	Q	U	M	E	I	I	R	Z	S
F	V	Q	V	F	A	A	M	Q	O	N	N	P	T	X
Q	T	K	R	U	S	D	E	N	Y	T	B	F	S	X
E	N	W	J	A	R	Z	A	Y	Y	E	L	G	I	M
G	E	R	J	M	L	T	U	O	H	R	Q	Q	H	Z
A	I	A	O	T	N	V	M	G	U	C	B	Y	R	Y
L	L	B	H	U	O	L	A	Z	G	E	J	O	P	N
F	C	W	C	N	R	M	L	Z	Y	P	G	U	Y	O
I	W	U	K	N	M	V	E	P	B	T	N	E	H	V
N	T	M	G	E	E	V	F	D	Y	I	U	F	T	K
E	R	B	X	L	W	Z	I	Y	M	O	R	E	T	Q
R	X	I	P	D	P	A	Q	D	J	N	Q	R	P	V
W	W	L	J	H	A	T	U	H	G	B	E	A	S	I
K	T	S	V	R	Z	E	E	H	E	S	C	P	A	L

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

4 horizontal: CLIENTVPN Réseau privé virtuel chiffré. (9 lettres)

5 horizontal: JUMEAUMALEFIQUE Point d'accès malveillant imitant un réseau Wi-Fi. (15 lettres)

6 horizontal: HTTPS Transmission web sécurisée. (5 lettres)

7 horizontal: RENIFLAGE Capture des paquets de données réseau. (9 lettres)

8 horizontal: TUNNEL Chemin sécurisé des données en transit. (6 lettres)

VERTICALEMENT

1 vertical: PAREFEU Filtrage du trafic entrant. (7 lettres)

2 vertical: INTERCEPTION Lecture du trafic en transit. (12 lettres)

3 vertical: NORMEWPA Norme moderne de sécurité Wi-Fi (WPA3). (8 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. TCPRNEIIOTNE — **INTERCEPTION**
2. UUEMMAQJEUEFILA — **JUMEAUMALEFIQUE**
3. CTNLVNEPI — **CLIENTVPN**
4. MPAWENOR — **NORMEWPA**
5. AFEELIRGN — **RENIFLAGE**
6. PHTST — **HTTPS**
7. ETNLNU — **TUNNEL**
8. AEUPEFR — **PAREFEU**

CORRIGÉ DU DÉFI DU CODE SECRET

"CHIFFREZ LE TRAFIC WIFI PUBLIC AVEC UN VPN"

Corrigé des études de cas

A Étude de cas 1 : Contenir l'interception de paquets sur un Wi-Fi public

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un commercial à distance, connecté à un réseau Wi-Fi public d'aéroport, remarque que plusieurs e-mails professionnels sensibles ont fuité peu après leur envoi en clair.
- Stratégie et solution recommandées : imposez l'utilisation d'un client VPN d'entreprise sur tous les postes de travail distants. Imposez des extensions de navigateur HTTPS uniquement et bloquez les protocoles non chiffrés (comme HTTP et FTP) au niveau du pare-feu du client.

B Étude de cas 2 : Défense contre les faux points d'accès Evil Twin

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : des attaquants déploient un point d'accès sans fil malveillant nommé 'CoffeeShop_Guest' qui imite le point d'accès légitime d'un café et capturent le trafic réseau des clients qui ne se doutent de rien.
- Stratégie et solution recommandées : auditer les adresses MAC BSSID des points d'accès pour vérifier l'authenticité du réseau. Imposer la validation de la conformité des clients pour bloquer la connexion aux réseaux ouverts et exiger des points d'accès cellulaires pour le travail sensible.